IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

INVENTORS: **Xiaowen YANG**

CASE: **YANG 1**
TITLE: **SCRAMBLE METHODS AND APPARATUS FOR PACKETIZED DIGITAL VIDEO SIGNAL IN CONDITIONAL ACCESS SYSTEM**

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

Enclosed are the following papers relating to the above-named application for patent:

Specification (including claims and Abstract) - 20 pages
5 Informal sheets of drawing(s)
1 Assignment with Cover Sheet
Declaration and Power of Attorney

CLAIMS AS FILE				
	NO. FILED	NO. EXTRA	RATE	CALCULATIONS
Total Claims	22 - 20 =	2	x $18 =	$36
Independent Claims	7 - 3 =	4	x $78 =	$312
Multiple Dependent Claim(s), if applicable			$260 =	$0
Basic Fee				$690
			TOTAL FEE:	$1038

Please file the application and charge **Lucent Technologies Deposit Account No. 12-2325** the amount of **$1038** to cover the filing fee. Duplicate copies of this letter are enclosed. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 12-2325** as required to correct the error.

Please address all correspondence to **FARKAS & MANELLI, PLLC, 2000 M Street, N.W. 7th Floor, Washington, DC 20036-3307**, and all telephone calls to William H. Bollman at his Washington, DC local number of (202) 261-1000.

Respectfully submitted,

William H. Bollman
Reg. No.: 36,457
Attorney for Applicant(s)

Date: January 27, 2000

Farkas & Manelli, PLLC
2000 M Street, N.W. 7th Floor
Washington, DC 20036-3307
(202) 261-1000

APPLICATION UNDER UNITED STATES PATENT LAWS

Invention: **SCRAMBLE METHODS AND APPARATUS FOR PACKETIZED DIGITAL VIDEO SIGNAL IN CONDITIONAL ACCESS SYSTEM**

Inventor(s): Xiaowen YANG

Farkas & Manelli P.L.L.C.
2000 M Street, N.W.
7th Floor
Washington, D.C. 20036-3307
Attorneys
Telephone: (202) 261-1000

This is a:

[ ] Provisional Application

[X] Regular Utility Application

[ ] Continuing Application

[ ] PCT National Phase Application

[ ] Design Application

[ ] Reissue Application

[ ] Plant Application

SPECIFICATION

SCRAMBLE METHODS AND APPARATUS FOR PACKETIZED DIGITAL VIDEO SIGNAL IN CONDITIONAL ACCESS SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to the provision of subscription broadcast services. More particularly, it relates to a scrambling technique for a digital MPEG-2 data stream intended for proper reception by subscribers and scrambling for non-subscribers.

2. Background of Related Art

Subscription broadcast services for video and/or audio can be thought of as conditional access (CA) systems. In a conditional access system, a broadcast signal is actively scrambled for broadcast such that only authorized receivers can access the payload, e.g., video, audio and/or data, by descrambling the received scrambled signal.

An example conditional access system is a pay cable television channel, which is conditioned for proper reception by any particular user upon payment (i.e., subscription). Subscribers are permitted to descramble the received broadcast signal, while non-subscribers leave the signal scrambled.

Many scrambling techniques exist in conventional analog conditional access systems. For instance, an analog signal (e.g., analog video or analog audio) may be scrambled using: (1) a trap; (2) a reverse trap; (3) hidden channels; (4) sync attenuation or suppression; (5) variable delay line; (6) active line inversion; (7) active cut line rotation; (8) active line shuffle; or (9) reverse active line scan. Each of these conventional scrambling techniques are explained in a little more detail.

(1) Traps

A trap is a sharply tuned notch filter inserted in a subscriber's receive path at the point where the customer's service drop is taken from the network.

(2) **Reverse traps**

A reverse trap is an extra radio-frequency 'spoiler' signal inserted into that part of the frequency spectrum between the high frequency edge of the vision signal and the sound carrier.

(3) **Hidden channels**

A hidden channel uses a frequency channel over a cable which is not permitted for over-air broadcast use.

(4) **Sync attenuation or suppression**

Sync attenuation or suppression reduces the sync pulse amplitude of the radio-frequency signal by attenuation at the head end.

(5) **Variable line delay**

A variable delay device inserted in a receive path introduces various delays into some of the lines of the television picture video signal on a pseudo-random basis.

(6) **Active line inversion**

Active line inversion inverts the signal on the active line

(7) **Active cut line rotation**

Active cut line rotation (or active component rotation) relates to cutting the components on each line of the picture into two parts. The cut points are determined as part of a given encryption mechanism using a pseudo-ransom number generator. Each of the two parts is then interchanged (effectively rotated about the cut point) so that the line can be scrambled before transmission.

(8) **Active line shuffle**

Using active line shuffle, the line order of a video image in a line memory block is re-ordered so that errors will occur in the vertical direction. This is also called "Vertical scrambling". To implement active

line shuffle, a sufficient and significant amount of memory must be available in the line memory block of both the scrambler and the descrambler.

(9) **Reverse active line scan**

Reverse active line scan is performed by scanning the line from line end to line start, rather than in normal order from line start to line end. A pseudo-random sequence generator is used to assign the line for reversing the scan. Reverse active line scanning requires a one-line memory in both the scrambler and in each descrambler to store the active line for reverse scanning.

These scrambling techniques work adequately for analog broadcast systems by impairing the receive quality of a conditional access analog broadcast signal, but are not all applicable for use in the emerging digital broadcasts in conditional access systems.

For instance, MPEG-2 is an emerging digital compression standard which is gaining in popularity. MPEG-2 is a compression standard which allows the coding of studio quality video for digital TV, high-density CD-ROMs and TV-broadcasting. Generally, the signal exists in the Europe DVB (Digital Video Broadcast) system, US HDTV system, and other related fields. The present invention relates to the conditional access to a digital compressed MPEG-2 bitstream allowing only subscribers to properly receive the MPEG-2 bitstream, and presenting a scrambled signal to non-subscribers.

Fig. 5 shows a digital stream of MPEG-2 transport packets **520**.

In particular, in Fig. 5, the MPEG-2 transport packets **520** each contain a header portion **501, 503, 505, 507, 509**, and a payload portion **502, 504, 506, 508, 510** containing the underlying program data. According to MPEG-2, the MPEG-2 transport packets **520** are 188 bytes in length.

Using a MPEG-2 bitstream as defined in the appropriate standard (e.g., ISO/IEC 13818-1), no scrambling is allowed to be applied to the header portion **501**, **503**, **505**, **507**, **509** of any of the transport packets **520**. Moreover, according to the relevant standards, the length of the MEPG-2 transport packets must remain the same, i.e., 188 bytes.

These and other requirements limit the possible conventional scrambling techniques to, e.g., either (6) active line inversion, (7) active cut line rotation, (8) active line shuffle, or (9) reverse active line scan techniques, as described above.

Unfortunately, conventional scrambling techniques such as (6) to (9) described above require a significant amount of system resources. For instance, to invert an active line, perform active cut line rotation, or active line shuffling, the received image must first be unscrambled and/or unencrypted, and decompressed, before the image lines can be manipulated for scrambling purposes. This extra processing counteracts the efficiency of compressed digital transmissions, e.g., MPEG-2 compression, and generally wasting system resources. Moreover, no conventional scrambling technique makes use of the properties of a compressed digital signal, again wasting system resources.

There is a need for a technique and apparatus for efficiently scrambling a compressed digital data stream (e.g., MPEG-2) with appreciation of the compressed nature of the digital data stream and requiring minimal excess processing.

SUMMARY OF THE INVENTION

In accordance with the principles of the present invention, a device to descramble a packetized digital data stream comprises a receiver to receive a packet of a scrambled packetized digital data stream. The packet includes a header portion and a data payload. The data

payload includes a scrambled portion and a clear, unscrambled portion. A descrambler descrambles the scrambled portion of the data payload of the packet while leaving the clear, unscrambled portion unaffected.

A method of scrambling a packetized digital data stream in accordance with another aspect of the present invention comprises producing a data packet stream comprising a plurality of data packets. A first portion of a data payload of at least some of the plurality of data packets within the data packet stream are scrambled without scrambling a header of the at least some of the plurality of data packets.

A method of scrambling a packetized digital data stream in accordance with yet another aspect of the present invention comprises producing a data packet stream comprising a plurality of data packets. Every nth one of the plurality of data packets is scrambled, where n is an integer greater than 1, leaving remaining ones of the plurality of data packets unscrambled.

A method of descrambling a packetized digital data stream in accordance with still another aspect of the present invention comprises receiving a data packet stream comprising a plurality of data packets. Every nth one of the plurality of data packets is descrabled, where n is an integer greater than 1, leaving remaining ones of the plurality of data packets as received.

BRIEF DESCRIPTION OF THE DRAWINGS

Features and advantages of the present invention will become apparent to those skilled in the art from the following description with reference to the drawings, in which:

Fig. 1 shows a conditional access system including a broadcast scrambled or encrypted packetized data stream, e.g., an MPEG-2 video/audio bitstream.

Fig. 2 is a more detailed block diagram of the subscriber's receiving equipment including a descrambler/decrypter, in accordance with the principles of the present invention.

Fig. 3 shows a series of transport packets (e.g., five transport packets) of a digital, packetized bit stream (e.g., MPEG-2 bitstream), in accordance with the principles of the present invention.

Fig. 4 shows a partially scrambled or encrypted data payload portion inside a data payload portion of a data transport packet, in accordance with the principles of the present invention.

Fig. 5 shows a digital stream of MPEG-2 transport packets.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

The present invention relates a conditional access scrambling or encryption technique for a packetized digital data stream, e.g., a MPEG-2 bitstream, (1) by scrambling or encrypting the data payload of selective transport payload packets (e.g., every nth packet); (2) by scrambling or encrypting only a portion (e.g., a central portion) of the data payload of every transport payload packets; or (3) by both scrambling or encrypting the data payload of every nth packet and scrambling or encrypting only a portion of the data payload of every transport payload packet.

With advance knowledge by the subscriber's descrambler of which payload packets are being scrambled, and/or of which portion of which payload packets, descrambling can be performed with minimal processing and without the need to first recreate the underlying image and/or audio.

Fig. 1 shows a conditional access system including a broadcast scrambled or encrypted packetized data stream, e.g., an MPEG-2 video/audio bitstream **120**.

In particular, in Fig. 1, the scrambled MPEG-2 bitstream can be broadcast or transmitted using any applicable technique, e.g., from a headend of a cable system, or from an RF transmitter of a wireless system.

The conditional access system includes one or more non-subscribers **125** as well as one or more subscribers **100**. The subscriber's receiving equipment **100** includes a descrambler to descramble the scrambled/encrypted MPEG-2 digital video/audio bitstream **120** transmitted or broadcast system wide.

Fig. 2 is a more detailed block diagram of the subscriber's receiving equipment **100** including a descrambler/decrypter **202**, in accordance with the principles of the present invention.

In particular, in Fig. 2, the broadcast scrambled/encrypted MPEG-2 digital video and/or audio signal is descrambled by a descrambler/decrypter **202**, and decoded by an appropriate digital compression decoder **206** (e.g., an MPEG-2 decoder), and output as a clear digital video and/or audio signal for use by the user. For instance, the clear digital video and/or audio signal may be provided to a television set or stereo receiver for viewing/listening by the user.

The subscriber's receiving equipment **100** further includes a controller **204**, which generally controls the operations of the subscriber's receiving equipment **100**. The controller **204** may be, e.g., a microprocessor, a microcontroller, or a digital signal processor (DSP). In the disclosed embodiment, the controller coordinates the descrambling/decrypting of the received scrambled MPEG-2 compressed digital video/audio signal, as well as the decoding of the unscrambled but still compressed video and/or audio signal.

While the descrambler **202** and MPEG-2 decoder **206** are shown separate from the controller **204** in Fig. 2, the descrambler **202**

and/or the MPEG-2 decoder **206** may be integrated within the program memory of the controller **204** within the principles of the present invention.

The descrambler/decrypter **202** (and corresponding scrambler/encrypter at a broadcasting location) utilize a digital scrambling technique which leaves a header portion of all transport data packets unaffected, and also maintains the specified length of the transport data packets (e.g., at 188 bytes in accordance with MPEG-2 standards).

In particular, in accordance with the principles of the present invention, the descrambler **202** descrambles either (1) by descrambling or decrypting the data payload of selective transport payload packets (e.g., every nth packet); (2) by descrambling or decrypting only a portion (e.g., a central portion) of the data payload of every transport payload packets; or (3) by both descrambling or decrypting the data payload of every nth packet and descrambling or decrypting only a portion of the data payload of every transport payload packet. A corresponding scrambler within the headend equipment performs the complementary scrambling or encryption process.

(1) Scramble/Encrypt one transport packet payload in every n packets

In accordance with this digital packetized signal scrambling/encryption technique capable of providing conditional access to a compressed digital signal scrambles the data payload portion of every nth transport packet, n being an integer greater than 1.

Fig. 3 shows a series of transport packets (e.g., five transport packets) of a digital, packetized bit stream (e.g., MPEG-2 bitstream).

In particular, in Fig. 3, a digital bitstream **402-410** corresponding to an underlying video and/or audio signal is scrambled by

scrambling the data payload portions **402a**, **410a** of every nth (e.g., every 4th as shown in Fig. 3) transport packet **402**, **410**.

Preferably, the particular transport packets **402**, **410** chosen (and therefore the value of n) is selected to cause a sufficient amount of damage or scrambling to the received image and/or audio to cause the received signal to be unwatchable or unlistenable to non-subscribers. However, subscribers, having advance knowledge of the particular transport packets **402**, **406** and the portion of the data payload **402a**, **410a** which is scrambled, can adequately reverse or descramble the scrambling, and therefore properly recover the data payload of all transport packets.

As an example of the selection of the value of n, an embodiment will be described with reference to a compressed, packetized digital bitstream used for video broadcast signals. In particular, in a DVB or GA high definition television (HDTV) system, the frame order of the picture in the coded bitstream is the order in which the decoder processes the frames. The original or reconstructed frames are not necessarily in the correct order for display. At the source encoder input and the decoder output, the frame order is:

```
1  2  3  4  5  6  7  8  9 10 11 12 13
I  B  B  P  B  B  P  B  B  I  B  B  P
```

At the encoder output, in the coded bitstream, and at the decoder input, the frame order is:

```
1  4  2  3  7  5  6 10  8  9 13 11 12
I  P  B  B  P  B  B  I  B  B  P  B  B
```

Picture '1I' is used to form a prediction for picture '4P'. Picture '4P' and '1I' are both used to form predictions for pictures '2B' and '3B'. The 'I' frame is the base of the 'P' and 'B' frames.

In accordance with the principles of the present invention, sufficient scrambling will be accomplished by scrambling every other I frame. Sufficient scrambling is accomplished because proper decoding requires two I frame detect mechanisms.

Thus, by scrambling or encrypting one transport packet in every n packets (e.g., one I frame in every 12 transport packets), the picture information base, that is I and P frame, will both be 'damaged' to provide a scrambled signal. Therefore, an unauthorized decoder will be unable to decode the underlying HDTV video image picture even if the remaining n-1 frames (e.g., the remaining 11 frames) are in clear!

(2) Partially Scramble/Encrypt data payload of every (or every nth) transport packet:

Another scrambling/encryption technique suitable for use in scrambling digital packetized data (especially compressed image and/or audio data) in accordance with the principles of the present invention partially scrambles the data payloads of all received data transport packets. Although the principles relate to the scrambling of the entire contents of all data payloads, such excess scrambling may cause the need for a significant amount of processing to receive the digital signal, counteracting reasons for using a compressed digital signal in the first place. Thus, it is preferred that only a portion of each data payload be scrambled, e.g., a portion including a central portion of a data packet.

Fig. 4 shows a partially scrambled or encrypted data payload portion **306** inside a data payload portion **320** of a data transport packet **300**. For explanation purposes, Fig. 4 is shown to have a length corresponding to MPEG-2. However, the principles of the present

invention relate to the scrambling of any digital standard transported in packets over a conditional access system.

In particular, in Fig. 4, only a portion **306** of a data payload portion **320** of each transport packet **300** is scrambled or encrypted using any suitable technique (e.g., invert all bits, reverse order of bits, etc.), leaving the header **302** of the transport packet **300** clear and unaffected. In the preferred embodiment, a significant portion **304**, **308** of the data payload portion **320** is left clear and unscrambled. Moreover, in the preferred embodiment, the scrambled portion **306** includes a central point of the data payload portion **320**.

Both the scrambler and the descrambler are coordinated with respect to which transport packets are scrambled and/or as to which portion of a given transport packet is scrambled. This information may be fixed for a given subscriber, for a given channel, or for a given conditional access system. Alternatively, the particular portions being scrambled (and the particular scrambling technique used) may be passed to subscribers either in the header portion **302** of scrambled transport packets, and/or as separate control information.

How and why the partial scrambling of a data payload works to suitably scramble a digital signal is explained with reference to an MPEG-2 bitstream.

In particular, using an MPEG-2 bitstream transport packet as an example as shown in Fig. 4, the underlying video/audio signal carried in the data payload portion **320** is in compressed form. The structure of the underlying compressed video signal in compliance with the relevant MPEG-2 standards is generally divided into 6 levels, from the top to the bottom described as:

- Sequence
- Group of Pictures
- Pictures

- Slices
- Macroblocks
- Blocks

The lowest level of the elementary stream synchronization is the slice. There is no error correcting for the video compressed data stream in the source coding. Therefore, when the MPEG-2 decoder **206** decodes the underlying video stream, it will discard the entire slice in which unrecoverable errors occur or if the decoder **206** can't find the slice_start_code in the slice structure.

If only a few slices are discarded, an image with satisfactory quality can still be recovered, or at least the degradation or 'damage' to the image may be unperceivable by the user because the decoder **206** can replace the discarded slices with an adjacent slice. The slice replacement may be fine, especially when the image contains little movement from one frame to the next. Even if there is a large amount of movement, the effect of just a few slice replacements will be discounted by the viewer. Thus, when only a few slices are scrambled, adequate scrambling making the signal unusable by non-subscribers may not be accomplished.

However, if many slices are caused to be discarded by scrambling (e.g., half of all the slices in a picture (or in the group of picture, sequence)), the resulting picture will be unwatchable. In this case, adequate scrambling will have been accomplished.

In accordance with the principles of the present invention, the 2_bits_transport_scrambling_control flag in the transport packet link header **302** is set to '10' or '11'. In that transport packet **300**, only part **306** of the data payload **320** is scrambled.

The scrambled portion **306** is preferably centered in the data packet, but may be at any portion of the data payload **320** within the principles of the present invention. Moreover, the scrambled portion **306**

may be at a fixed location within each transport data packet, or may move in location from transport data packet to transport data packet.

For instance, selecting a central point in the data payload, the scramble location can shift +/- n bytes from that central point. Of course, it is preferred that the shift information be coordinated between scrambler and descramblers.

While the length of the scrambled portion **306** may change, it is preferred that the length of the scrambled portion **306** remain fixed, even when shifting location from data packet to data packet. Moreover, the length of the scrambled portion should be selected based on the desired amount of scrambling of the received signal, keeping in mind that the larger the length of the scrambled portion **306**, the greater the need for descrambling operation memory. Thus, there is a design balance to be struck as between an amount of damage caused to a scrambled digital packetized signal, and an acceptable amount of descrambling overhead to be incurred.

Selection of a central point in the transport packet **300** is intended to allow blind placement of a scrambled portion within the data payload without the need to process header and/or data payload information. Thus, it is presumed that the central point in the transport packet **300** is well within the data payload portion **320**.

The scrambled portion **306** of the data transport packet **300** may be scrambled using any suitable technique applicable to data, e.g., inverse, cut point rotation, etc., or encrypted by a certain block or series encryption algorithm like DES. A suitable simple technique is to invert the data in the scrambled portion **306**. Using a suitable scrambling technique, the data contained in the relevant slice of the picture or the slice_start_code will be destroyed, and an ordinary decoder which has not been authorized by the broadcaster (i.e., a non-subscriber) will discard such slices. As a result, the unauthorized viewer will be unable to enjoy

the program that they haven't paid for. On the other hand, all authorized receivers **100** including a suitable descrambler/decrypter **202** will have knowledge of the appropriate transport packets and/or particular scrambled portions of the transport packets such that the program slice structure can be corrected to a normal state, allowing the subsequent MPEG-2 decoder **206** to decode the video/audio bitstream normally without discarded slices.

The new scramble techniques and apparatus in accordance with the principles of the present invention maintain the advantages of the user of a compressed digital signal, e.g., MPEG-2 digital compressed signal characteristics, within the relevant requirements for standard digital transmissions and without the need for substantial additional system resources. For instance, scrambling of data payloads of transport packets in a conditional system in accordance with the principles of the present invention requires less RAM and lower decryption system operational speeds as compared to otherwise conventional techniques. Moreover, because of the lowered operational speeds required, a more sophisticated encryption algorithm may be performed. The new scrambling technique is difficult to hack, attracting potential customers and increasing the appeal of the scrambling technique.

In accordance with the principles of the present invention, at best only part of an underlying video image (or audio signal) can be properly received by non-subscribers to a conditional access system, providing adequate scrambling to those non-subscribers.

While the invention has been described with reference to the exemplary embodiments thereof, those skilled in the art will be able to make various modifications to the described embodiments of the invention without departing from the true spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A device to descramble a packetized digital data stream, comprising:

a receiver to receive a packet of a scrambled packetized digital data stream, said packet including a header portion and a data payload, and said data payload including a scrambled portion and a clear, unscrambled portion; and

a descrambler to descramble said scrambled portion of said data payload of said packet.

2. The device to descramble a packetized digital data stream according to claim 1, wherein:

said scrambled portion of said data payload is at a location within said payload portion of said packet such that said scrambled portion is preceded and succeeded by unscrambled portions within said packet.

3. The device to descramble a packetized digital data stream according to claim 1, wherein:

said digital data stream comprises an MPEG-2 digital data stream.

4. The device to descramble a packetized digital data stream according to claim 1, wherein:

said packet contains compressed digital data.

5. The device to descramble a packetized digital data stream according to claim 4, wherein:

said compressed digital data includes a video signal.

6. The device to descramble a packetized digital data stream according to claim 4, wherein:

said compressed digital data includes an audio signal.

7. The device to descramble a packetized digital data stream according to claim 4, wherein:

said compressed digital data includes a video signal and an audio signal.

8. A method of scrambling a packetized digital data stream, comprising:

producing a data packet stream comprising a plurality of data packets; and

scrambling a first portion of a data payload of at least some of said plurality of data packets within said data packet stream without scrambling a header of said at least some of said plurality of data packets.

9. The method of scrambling a packetized digital data stream according to claim 8, wherein:

said scrambling leaves a second portion of said data payload of each of said at least some of said plurality of data packets unscrambled.

10. A method of scrambling a packetized digital data stream, comprising:

producing a data packet stream comprising a plurality of data packets; and

scrambling every nth one of said plurality of data packets, where n is an integer greater than 1, leaving remaining ones of said plurality of data packets unscrambled.

11. The method of scrambling a packetized digital data stream according to claim 10, wherein:

said data packet stream is an MPEG-2 digital data stream.

12. The method of scrambling a packetized digital data stream according to claim 10, wherein said data packet stream comprises:

compressed video data.

13. The method of scrambling a packetized digital data stream according to claim 10, wherein said data packet stream comprises:

compressed audio data.

14. The method of scrambling a packetized digital data stream according to claim 10, wherein said data packet stream comprises:

compressed video data and compressed audio data.

15. A method of descrambling a packetized digital data stream, comprising:

receiving a data packet stream comprising a plurality of data packets; and

descrambling every nth one of said plurality of data packets, where n is an integer greater than 1, leaving remaining ones of said plurality of data packets as received.

16. The method for descrambling a packetized digital data stream according to claim 15, wherein said packetized digital data stream comprises:

MPEG-2 digital data.

17. Apparatus for scrambling a packetized digital data stream, comprising:

means for producing a data packet stream comprising a plurality of data packets; and

means for scrambling a first portion of a data payload of at least some of said plurality of data packets within said data packet stream without scrambling a header of said at least some of said plurality of data packets.

18. The apparatus for scrambling a packetized digital data stream according to claim 17, wherein said data packet stream comprises:

an MPEG-2 digital data stream.

19. Apparatus for scrambling a packetized digital data stream, comprising:

means for producing a data packet stream comprising a plurality of data packets; and

means for scrambling every nth one of said plurality of data packets, where n is an integer greater than 1, leaving remaining ones of said plurality of data packets unscrambled.

20. The apparatus for scrambling a packetized digital data stream according to claim 19, wherein said data packet stream comprises:

an MPEG-2 digital data stream.

21. Apparatus for descrambling a packetized digital data stream, comprising:

means for receiving a data packet stream comprising a plurality of data packets; and

means for descrambling every nth one of said plurality of data packets, where n is an integer greater than 1, leaving remaining ones of said plurality of data packets as received.

22. The apparatus for descrambling a packetized digital data stream according to claim 21, wherein said data packet stream comprises:

an MPEG-2 digital data stream.

ABSTRACT

A conditional access scrambling or encryption technique for a packetized digital data stream, e.g., a MPEG-2 bitstream, (1) by scrambling or encrypting the data payload of selective transport payload packets (e.g., every nth packet); (2) by scrambling or encrypting only a portion (e.g., a central portion) of the data payload of every transport payload packets; or (3) by both scrambling or encrypting the data payload of every nth packet and scrambling or encrypting only a portion of the data payload of every transport payload packet. With advance knowledge by the subscriber's descrambler of which payload packets are being scrambled, and/or of which portion of which payload packets, descrambling can be performed with minimal processing and without the need to first recreate the underlying image and/or audio.

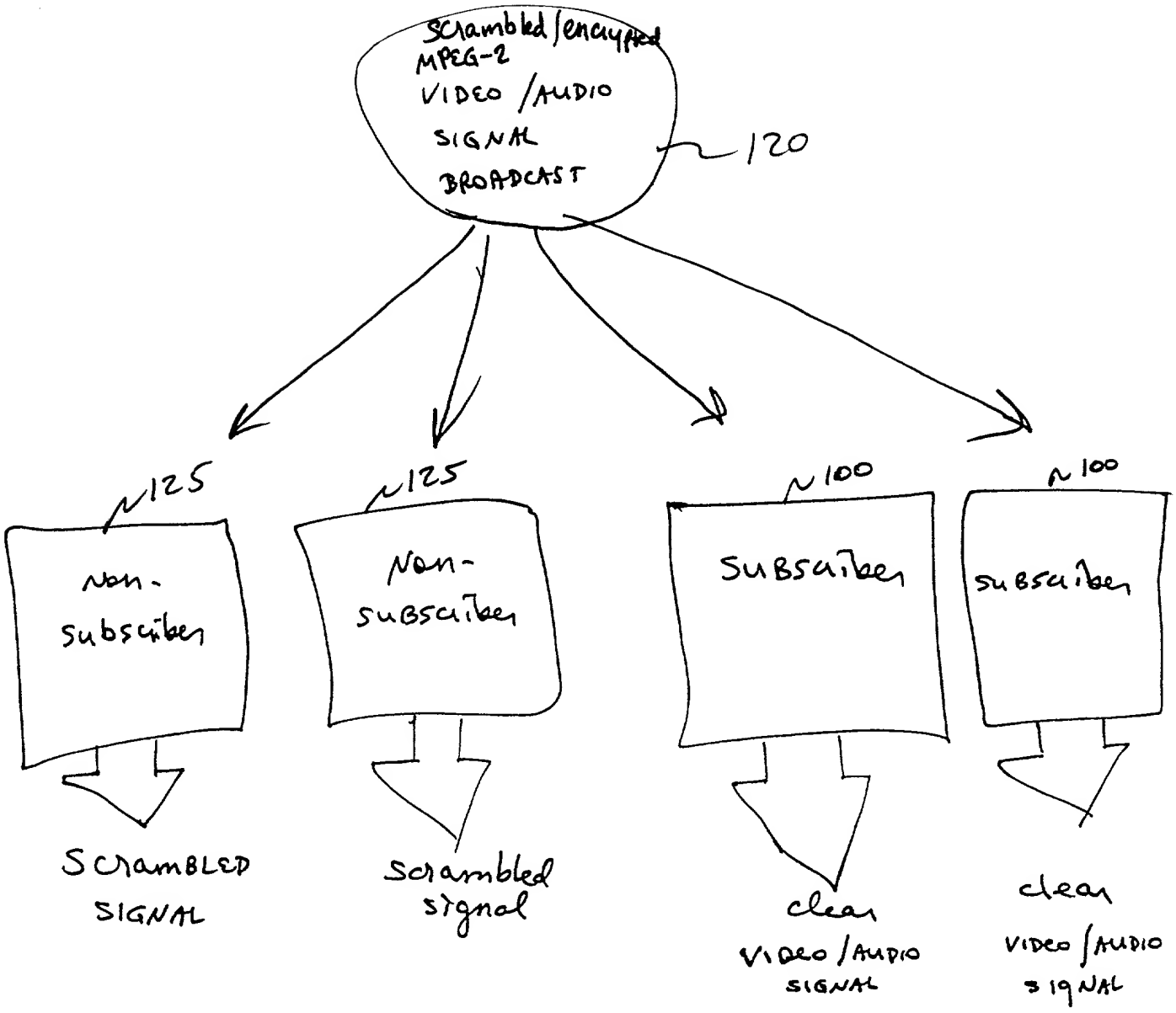

Scrambled/encrypted MPEG-2 VIDEO/AUDIO SIGNAL BROADCAST
120
125
Non-subscriber
SCRAMBLED SIGNAL
125
Non-subscriber
scrambled signal
100
subscriber
clear VIDEO/AUDIO SIGNAL
100
subscriber
clear VIDEO/AUDIO SIGNAL

FIG. 1

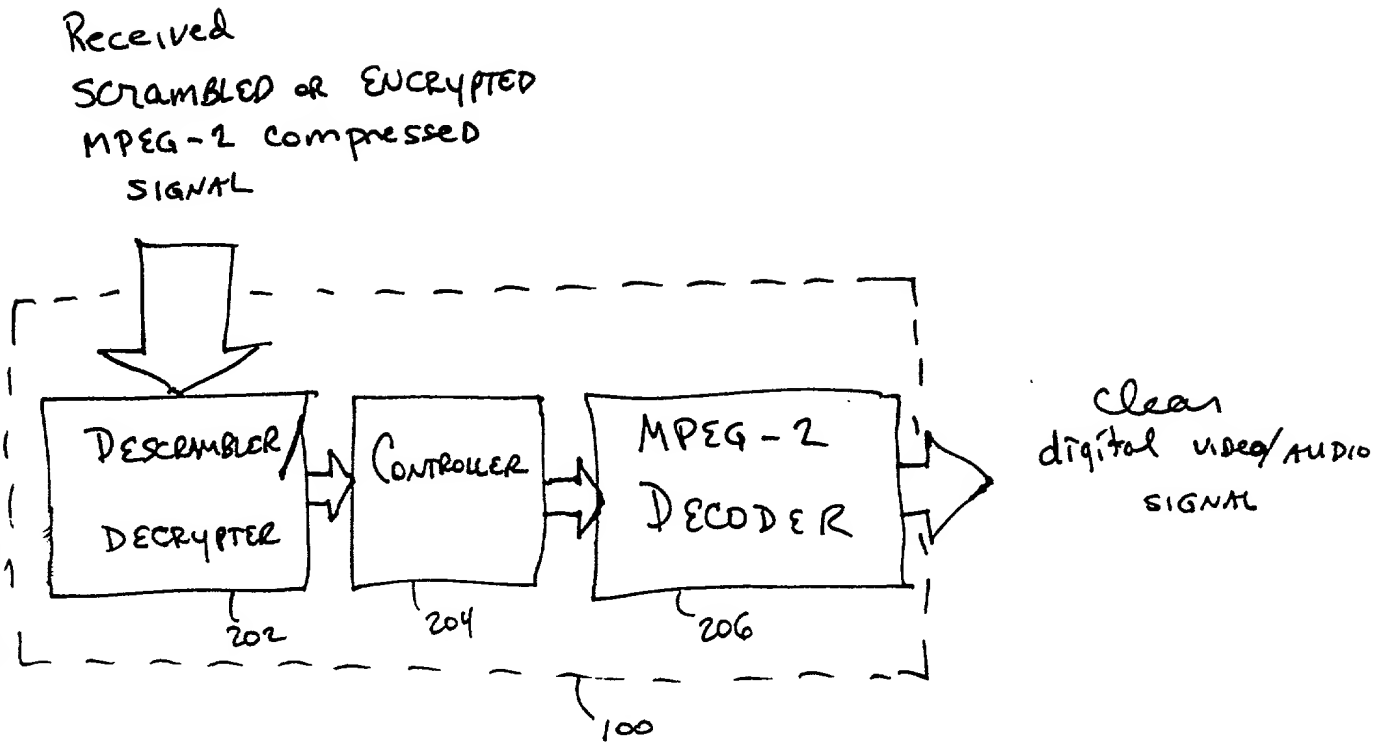
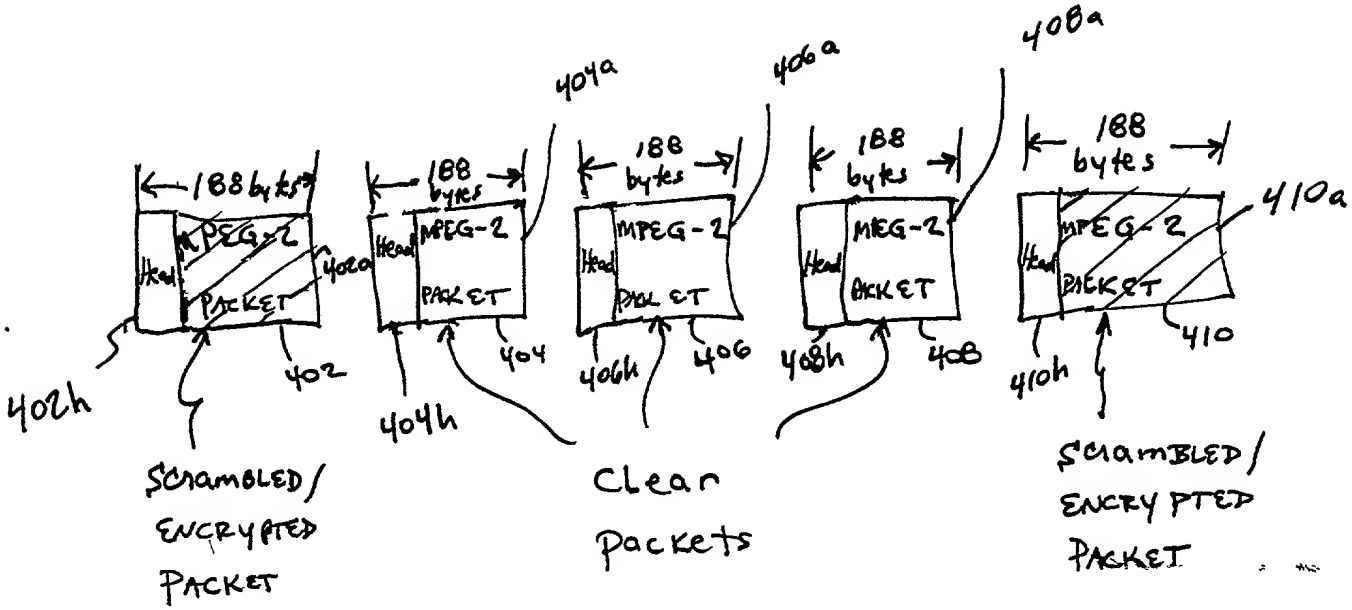
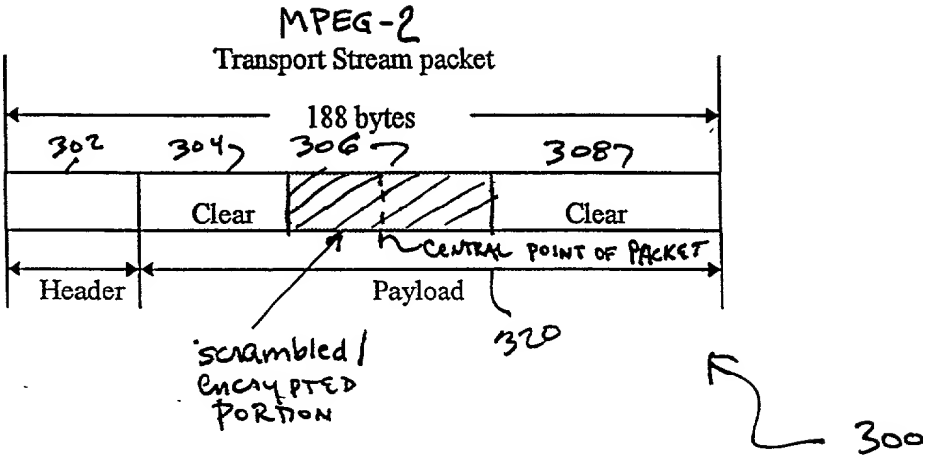

Received
SCRAMBLED or ENCRYPTED
MPEG-2 compressed
SIGNAL
DESCRAMBLER
DECRYPTER
CONTROLLER
MPEG-2
DECODER
clear
digital video/AUDIO
SIGNAL
202
204
206
100

FIG. 2



Fully Scramble or Encrypt
every N^{th} MPEG-2
PACKET

FIG. 3



Partially Scramble or Encrypt the Payload

FIG. 4

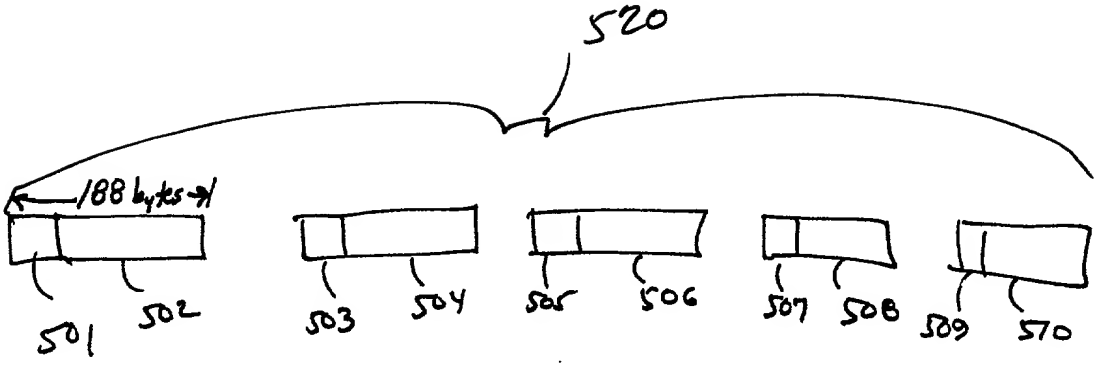


FIG. 5

PRIOR ART

YANG 1 (657)

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney

As the below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **SCRAMBLE METHODS AND APPARATUS FOR PACKETIZED DIGITAL VIDEO SIGNAL IN CONDITIONAL ACCESS SYSTEM** the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to in this oath or declaration.

I acknowledge the duty to disclose all information known to me which is material to patentability as defined in Title 37, Code of Federal Regulations, 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

None

I hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

None

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Lester H. Birnbaum	(Reg. No. 25830)
Richard J. Botos	(Reg. No. 32016)
Jeffery J. Brosemer	(Reg. No. 36096)
Kenneth M. Brown	(Reg. No. 37590)
Craig J. Cox	(Reg. No. 39643)
Donald P. Dinella	(Reg. No. 39961)
Guy Eriksen	(Reg. No. 41736)
Martin I. Finston	(Reg. No. 31613)
James H. Fox	(Reg. No. 29379)
William S. Francos	(Reg. No. 38456)
Barry H. Freedman	(Reg. No. 26166)
Julio A. Garceran	(Reg. No. 37138)
Mony R. Ghose	(Reg. No. 38159)
Jimmy Goo	(Reg. No. 36528)
Anthony Grillo	(Reg. No. 36535)
Stephen M. Gurey	(Reg. No. 27336)
John M. Harman	(Reg. No. 38173)
Michael B. Johannesen	(Reg. No. 35557)
Mark A. Kurisko	(Reg. No. 38944)
Irena Lager	(Reg. No. 39260)
Christopher N. Malvone	(Reg. No. 34866)
Scott W. McLellan	(Reg. No. 30776)
Martin G. Meder	(Reg. No. 34674)
John C. Moran	(Reg. No. 30782)
Michael A. Morra	(Reg. No. 28975)
Gregory J. Murgia	(Reg. No. 41209)
Claude R. Narcisse	(Reg. No. 38979)
Joseph J. Opalach	(Reg. No. 36229)
Neil R. Ormos	(Reg. No. 35309)
Eugen E. Pacher	(Reg. No. 29964)
Jack R. Penrod	(Reg. No. 31864)
Daniel J. Piotrowski	(Reg. No. 42079)
Gregory C. Ranieri	(Reg. No. 29695)
Scott J. Rittman	(Reg. No. 39010)
Eugene J. Rosenthal	(Reg. No. 36658)
Bruce S. Schneider	(Reg. No. 27949)
Ronald D. Slusky	(Reg. No. 26585)
David L. Smith	(Reg. No. 30592)
Patricia A. Verlangieri	(Reg. No. 42201)
John P. Veschi	(Reg. No. 39058)
David Volejnicek	(Reg. No. 29355)
Charles L. Warren	(Reg. No. 27407)
Jeffrey M. Weinick	(Reg. No. 36304)

Eli Weiss (Reg. No. 17765)

I hereby appoint the attorney(s) on ATTACHMENT A as associate attorney(s) in the aforementioned application, with full power solely to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected with the prosecution of said application. No other powers are granted to such associate attorney(s) and such associate attorney(s) are specifically denied any power of substitution or revocation.

Full name of the sole inventor: **Xiaowen YANG**

Inventor's signature Yang Xiaowen Date Jan. 24, 2000

Residence: **Shanghai, People's Republic of China**

Citizenship: **CHINA**

Post Office Address: ~~**No. 30, Room 204, Lane 112, Datong Road, Caoqiao, Shanghai, China 200137**~~

My Post Office (Home) Address changed to:

Room 1003, No. 37, Lane 380, Tian Yao Qiao Road,

Shanghai, China, 100030

ATTACHMENT A

Attorney Name(s): William H. Bollman Reg. No.: 36,457

Telephone calls should be made to **Farkas and Manelli PLLC** at:

Phone No.: 202-261-1000

Fax No.: 202-887-0336

All written communications are to be addressed to:

Farkas & Manelli pllc
2000 M Street, N.W.
7th Floor
Washington, D.C. 20036-3307